TO: [Company Name]

Street: [Company address]

Postal code PO-Box: [Company Postal code /PO-Box]

Country: [Company HQ]

Outsourcing Illegality: How Governments Push Unlawful Rules onto Private Platforms

[Location], August 6, 2025

LEGAL NOTICE – BINDING DISCLOSURE

Notice to Agents and Principals: This document serves as formal notice to all agents, representatives, and intermediaries acting on behalf of any entity addressed herein. Receipt of this communication by any agent is legally equivalent to receipt by the principal. All responsibilities, liabilities, and obligations conveyed in this notice are hereby binding upon both.

DECLARATION OF NON-CONSENT – LEGAL ADDENDUM

You are hereby notified that I do **not consent** to any and all implied, explicit, or presumed agreements, associations, contracts, jurisdictions, or obligations that have not been voluntarily, knowingly, and expressly entered into by me. Any attempt to bind me to terms, conditions, authorities, or processes without my informed and written consent is strictly refused and rebutted.

I reject:

- Any presumption of authority over my natural rights
- Any implied acceptance through silence, inaction, or receipt
- Any construct of legal fiction used to override sovereignty or lawful standing

This declaration applies unconditionally and retroactively to any engagement prior to this notice, and prospectively from the date of receipt. Any failure to rebut this declaration constitutes tacit agreement to the terms herein.

This notice forms part of the formal objection as presented. I reserve all rights, waiving none.

LEGAL NOTICE OF NON-COMPLIANCE

Subject:
Unlawful Processing of Biometric Data,
Coercive Bundling,
Unauthorised System Access
Third-Party Interference with Contracts under European and Dutch Law

Date: August 6, 2025

Declarant Information:
Full Name: [Your Full Name]
Address: [Your Address]
Email: [Your Email]
Phone: [Your Phone Number]

I. INTRODUCTION

This notice serves as a formal declaration of legal non-compliance with European Union and Dutch legislation. It addresses unlawful digital practices including:

- Unauthorised collection and processing of biometric data
- Coercive bundling of digital services ("tying")
- Unauthorised system access and behavioural surveillance
- Third-party interference with existing contractual relations

These practices violate fundamental rights under EU law and shall give rise to civil, administrative, and criminal liability.

II. APPLICABLE LEGAL FRAMEWORK

A. Data Protection and Privacy

Key Legal Sources on Biometric Data and Digital Rights

This section outlines the most relevant legal instruments governing biometric data, privacy, and digital rights within the EU framework.

1) GDPR (EU 2016/679)

- Key Articles: 4(14), 5, 9(1)–(2)(a)
- Clarification: Defines *biometric data* and prohibits its processing without explicit, informed consent.

2) Law Enforcement Directive

- Key Articles: 6, 10
- Clarification: Sensitive data may only be processed when strictly necessary and proportionate to the purpose.

3) EU Charter of Fundamental Rights

- Key Articles: 7, 8, 11, 16, 47, 52

- Clarification: Enshrines rights to privacy, data protection, freedom of expression, freedom to conduct a business, and judicial remedy. Article 52 sets limits on rights restrictions.

4) EDPB Guidelines 05/2022

- Key Provision: —
- Clarification: Recommends bans on biometric identification/emotion inference in public spaces.

5) EU AI Act (EU 2024/1689)

- Key Articles: Article 5, Annex III
- Clarification: Prohibits untargeted biometric categorization and identifies high-risk biometric AI systems requiring strict oversight.

B. Consumer Protection and Market Conduct

Legal Framework on Coercive Bundling, Consumer Rights, and Platform Conduct

This section outlines key EU and Dutch legal sources addressing unfair commercial practices, bundling, and user rights in digital services.

1) TFEU Article 102

- Key Provision: —
- Clarification: Prohibits abuse of dominant market position, including coercive tying of services.

2) Dutch Competition Act (Article 24)

- Key Provision: —
- Clarification: Serves as the national equivalent of TFEU Article 102, prohibiting similar dominance abuses.

3) Insurance Distribution Directive (2016/97)

- Key Provision: —
- Clarification: Prohibits forced bundling of insurance products with unrelated services or contracts.

4) Consumer Rights Directive (2011/83)

- Key Provision: —
- Clarification: Requires informed, fair, and transparent consent in consumer agreements and digital interactions.

5) Digital Markets Act (DMA – EU 2022/1925)

- Key Provision: Article 5
- Clarification: Prohibits gatekeepers from bundling services or restricting user choice, ensuring fair competition.

6) Dutch Civil Code

- Key Articles: 193b–193d, 162
- Clarification: Prohibits unfair commercial practices and establishes liability for unlawful acts, including contractual interference.

7) E-Commerce Directive

- Key Articles: 5–7
- Clarification: Requires transparency in digital services and limits intermediary liability under specific conditions.

III. CRIMINAL LAW AND SYSTEM ACCESS

Criminal Code Articles and Digital Offenses

1) Article 138ab Dutch Criminal Code — Computer Intrusion

Covers unauthorised access to computer systems, script injection, browser manipulation, and adblocker scanning.

2) Article 138 Sr — Digital Trespass

Applies to user environments treated as private domains, for example personal accounts or interfaces.

3) Article 326 Sr — Fraud and Deception

Includes misleading consent mechanisms and deceptive interface design intended to manipulate user decisions.

4) Article 225 Sr — Forgery

Covers falsified consent records and manipulated system logs.

5) Article 227b Sr — Withholding Information

Relates to the non-disclosure of behavioural tracking systems and profiling mechanisms.

6) Article 365 Sr — Abuse of Authority

Concerns the misuse of digital platforms to influence or manipulate user behaviour.

7) **Article 273f Sr — Human Exploitation**

Applies to coercive biometric control or manipulation, especially when used to extract compliance.

8) **Article 284 Sr — Coercion**

Includes the use of bundling and forced consent mechanisms to pressure users into agreement.

IV. CYBERSECURITY AND SYSTEM ACCESS LAW

Key Legal Sources on Cybercrime and Digital Regulation

1) **Directive 2013/40/EU — Attacks Against Information Systems**

Establishes criminal penalties for illegal access to systems, interference with system integrity, and data tampering. It harmonizes cybercrime laws across EU member states.

2) **EU Cybersecurity Act (Regulation EU 2019/881)**

Introduces EU-wide cybersecurity certification schemes, sets minimum security standards, and mandates incident reporting for critical infrastructure and digital services.

3) **NIS2 Directive (Directive EU 2022/2555)**

Expands security and reporting obligations for essential and important entities, including cloud providers, data centres, and digital platforms. Strengthens risk management and supply chain oversight.

4) **Budapest Convention on Cybercrime**

The first international treaty on cybercrime, providing a legal framework for criminalizing unlawful access, data interception, and enabling cross-border cooperation in investigations and prosecutions.

V. CROSS-JURISDICTIONAL MAPPING

Comparative Legal Overview: Dutch, EU, and Conceptual Equivalents

1) **Unauthorised System Access**

- Dutch Law: Article 138ab Sr
- EU / International Law: Directive 2013/40/EU, Budapest Convention

- Conceptual Equivalent: Illegal system intrusion This refers to unauthorised entry into digital systems, including hacking, script injection, and bypassing access controls.

2) Digital Privacy Rights

- Dutch Law: Article 138 Sr
- EU / International Law: EU Charter of Fundamental Rights (Articles 7–8), NIS2 Directive
- Conceptual Equivalent: Digital trespass Protects the integrity of private digital environments, for example personal accounts and user interfaces, from unauthorised interference.

3) Data Protection Violations

- Dutch Law: GDPR, Article 162 BW (Civil Code)
- EU / International Law: GDPR, Charter Articles 7–8
- Conceptual Equivalent: Unlawful biometric processing Covers misuse of personal and biometric data, including unauthorised collection, profiling, or retention.

4) Coercive Bundling

- Dutch Law: Civil Code Articles 193b–193d, Digital Markets Act (DMA)
- EU / International Law: DMA Article 5, TFEU Article 102
- Conceptual Equivalent: Market abuse Refers to practices where users are forced to accept bundled services or conditions, often under monopolistic or dominant market behaviour.

5) Misleading Mechanisms

- Dutch Law: Article 326 Sr
- EU / International Law: GDPR Recital 39, Consumer Rights Directive, Unfair Commercial practices Directive (UCPD)
- Conceptual Equivalent: Deceptive commercial behaviour Includes dark patterns, misleading consent mechanisms, and manipulative interface design techniques that distort user choice.

6) Contractual Interference by Third Parties

- Dutch Law: Article 162 BW
- EU / International Law: Tortious interference principles (EU civil law)

- Conceptual Equivalent: Inducing breach or obstructing contract execution Covers situations where third parties unlawfully disrupt or manipulate contractual relationships between others.

V-A. ADDITIONAL LEGAL FRAMEWORK: THIRD-PARTY INTERFERENCE

Certain external entities not party to an existing contract, have knowingly interfered with its execution, inducing breach or obstructing performance. This triggers liability under:

- **Dutch Civil Code (Art. 6:162 BW)**: A third party that causes a contractual breach through intentional and unlawful actions may be held liable under tort law.
- **European Legal Principles** (e.g. PECL Art. 6:111): Third-party interference is considered unlawful if there is knowledge of the contract and intentional disruption.
- **EU Charter of Fundamental Rights**: Protection of freedom to conduct business (Art. 16) and access to legal remedies (Art. 47) extends to unjust disruptions by external agents.

These provisions support legal recourse against parties who seek to disrupt consent-based service contracts or initiate intrusive conduct that voids prior agreements.

VI. IMPROPER INVOCATION OR UNLAWFUL RELIANCE OF LEGITIMATE INTEREST CLAIMS

Numerous data controllers purport to rely upon GDPR Art. 6(1)(f) to justify intrusive surveillance or monetization. However, as clarified by the CJEU in *Rīgas satiksme* (C-13/16), legitimate interest requires a demonstrable balancing test and cannot justify intrusive tracking without safeguards:

- Legitimate interest must not override user rights
- A documented balancing test is required
- Less intrusive legal bases should be preferred

Common violations include:

- Misleading “Accept All” buttons
- Obstructive opt-out flows
- Structurally coercive consent mechanisms masking data harvesting

These tactics violate GDPR principles and may constitute *computervredebreuk* under Dutch law when paired with unauthorised system access or coercive bundling.

VII. RELEVANT CASE LAW

Key Legal Cases on Digital Rights and Cyber Conduct

1) *S. and Marper v. United Kingdom*

- Court: European Court of Human Rights (ECtHR)
- Year: 2008

- Relevance: Established that indefinite retention of biometric data (DNA, fingerprints) violates privacy rights under Article 8 ECHR. Introduced the principle of proportionality in biometric surveillance.

2) ***Schwarz v. Stadt Bochum***

- Court: Court of Justice of the European Union (CJEU)
- Year: 2013
- Relevance: Upheld the legality of fingerprint collection for passports under EU law, provided it meets proportionality and necessity standards.

3) ***UI v. Österreichische Post AG***

- Court: CJEU
- Year: 2023
- Relevance: Found that political profiling without valid consent violates GDPR. Reinforced strict standards for lawful data processing and transparency.

4) ***V.S. v. Ministerstvo***

- Court: CJEU
- Year: 2023
- Relevance: Clarified limits on biometric categorization and facial recognition. Emphasised that surveillance must be narrowly tailored and legally justified.

5) ***HR 15-12-2020, ECLI:NL:HR:2020:2036***

- Court: Dutch Supreme Court
- Year: 2020
- Relevance: Ruled that unauthorised automated access to a browser interface constitutes *computervredebreuk* (computer intrusion) under Dutch criminal law.

6) ***GS Media BV v. Sanoma***

- Court: CJEU
- Year: 2016
- Relevance: Established liability for hyperlinking to unlawful content when done knowingly. Set precedent for third-party responsibility in digital environments.

7) ***De Treek/Dexia***

- Court: Dutch Supreme Court
- Year: 2005

- Relevance: Addressed misleading contractual inducement and third-party liability for breach. Relevant to deceptive digital practices and platform accountability.

VIII. LEGAL CONSEQUENCES

A. Civil Liability

- Art. 162 BW: Unlawful act → damages
- Art. 193b BW: Misleading practices → declaratory relief
- WAMCA: Enables class actions for mass harm
- **Third-party interference**: Intentional breach inducement triggers tort liability

B. Regulatory Sanctions

- Dutch DPA: Fines up to €20M or 4% global turnover
- ACM: Coercive bundling and deceptive practices
- EU DPAs: Cross-border enforcement under GDPR, DMA, DSA

C. Criminal Penalties

- Art. 138ab Sr: Up to 2 years imprisonment
- Art. 273f Sr: Human exploitation via biometric profiling
- Art. 284 Sr: Coercion using forced consent structures

D. Ethical & Reputational Risks

- Loss of consumer trust
- Media scrutiny and reputational damage
- Market exclusion or blacklisting

IX. CONCLUSION & CALL TO ACTION

All implicated parties are hereby called upon to:

- Immediately cease all unlawful conduct
- Undertake a Data Protection Impact Assessment (DPIA) in full compliance with the GDPR
- Uphold contractual integrity and refrain from unauthorized third-party interference

Non-compliance shall result in:

- Civil proceedings pursuant to Article 6:162 BW (Dutch tort law)
- Regulatory sanctions, including fines under the GDPR and Digital Markets Act (DMA)
- Criminal prosecution under applicable provisions of the Dutch Penal Code

The aforementioned conduct constitutes a violation of the following legal frameworks and jurisprudence:

- Charter of Fundamental Rights of the European Union
- General Data Protection Regulation (GDPR)
- Dutch Civil Code and Dutch Penal Code
- Budapest Convention on Cybercrime

ADDENDUM: LEGAL ANALYSIS

- General Data Protection Regulation (GDPR)
- In the context of digital regulation, it is essential to understand how European legislation for example the **General Data Protection Regulation (GDPR)** and the **Digital Markets Act (DMA)** relate to practices involving data collection, profiling, and consent mechanisms[^1]. Gatekeepers under the DMA face stricter obligations, including a prohibition on bundling services without genuine user choice[^2].
- A key issue is the use of **biometric data**, for example facial recognition or fingerprint scanning, for identification or authentication. Under the GDPR, this data falls under special categories and requires explicit consent[^3]. The **European Data Protection Board (EDPB)** has clarified that such consent must be freely given, specific, and informed — and cannot be implied[^4].
- Another relevant legal basis is **legitimate interest** under Article 6(1)(f) GDPR. While it may justify certain processing activities, it requires a balancing test where the rights and freedoms of the data subject must outweigh the controller's interest, especially when sensitive data or tracking technologies are involved[^5].
- The use of **dark patterns** (manipulative interface design techniques) in consent mechanisms is also legally problematic. These manipulative design choices may constitute unfair commercial practices under the **Unfair Commercial Practices Directive**[^6], particularly when they mislead users or restrict their ability to make free choices.
- Under Dutch criminal law, **unauthorised computer access** is criminalized in Article 138ab of the Dutch Penal Code. The Supreme Court of the Netherlands has ruled that even automated access without consent falls within the scope of this provision[^7]. This is particularly relevant in cases involving system scanning or the deployment of tracking software without user permission.
- At the European level, the **Budapest Convention on Cybercrime** provides a framework for cross-border cooperation in digital crime enforcement[^8]. This treaty is especially relevant for international data flows and cloud-based services.
- Regarding **the automated processing of personal data relating to minors for behavioural targeting**, the **Digital Services Act (DSA)** prohibits targeted advertising based on personal data of minors, regardless of whether consent is obtained[^9]. This provision strengthens the protection of vulnerable groups online.

- Increasing judicial and regulatory scrutiny has emerged regarding **facial recognition** in **public spaces**. In recent case law, the Court of Justice of the European Union (CJEU) ruled that **biometric surveillance** must be **strictly necessary** and proportionate to be lawful[^10].

- Interference by **external parties** in **existing** contractual relationships can trigger civil liability under Dutch tort law. Article 6:162 BW allows for claims when a third party knowingly induces **breach or obstructs** performance of a **valid contract**[^11]. EU legal principles recognise tortious interference where there is intentional disruption and knowledge of the agreement[^12]. This is especially relevant where **consent-based** digital service agreements are **nullified or overridden** by platform operators or integrated external systems acting **outside contractual** scope.

[^1]: See GDPR (EU) 2016/679, especially Articles 4 and 6 for definitions and legal bases for processing.
[^2]: Regulation (EU) 2022/1925 (DMA), Article 5(2)(a)–(c): prohibits tying and bundling without user choice.
[^3]: GDPR Article 9(1): Biometric data used for identification is considered special category data. [^4]: EDPB Guidelines 05/2020 on Consent, §§40–45: explicit, informed, and freely given consent is required.
[^5]: CJEU, Case *C-13/16*, *Rīgas satiksme*, §§30–35: legitimate interest requires a careful balancing test.
[^6]: Directive 2005/29/EC, Annex I, points 20–23: misleading practices and coercive tactics are prohibited.
[^7]: Dutch Supreme Court, HR 15-12-2020, ECLI:NL:HR:2020:2036: automated access without consent qualifies as computer intrusion under Article 138ab.
[^8]: Council of Europe, *Budapest Convention on Cybercrime*, ETS No. 185.
[^9]: Regulation (EU) 2022/2065 (DSA), Article 28(3): profiling and targeted advertising using minors' personal data is prohibited.
[^10]: CJEU, Case *C-205/21*, Judgement of 30 January 2023: biometric surveillance must meet strict necessity and proportionality standards.
[^11]: Dutch Civil Code, Article 6:162 BW: unlawful act includes intentional interference in existing contracts.
[^12]: CJEU, Case C-610/15 (GS Media BV v. Sanoma), Judgement of 8 September 2016: third-party liability applies where unlawful interference is knowing and intentional.

FINAL CONCLUSION

The State must act solely in the context of legitimate dispute resolution, not as an architect of systemic data collection, behavioural control, or repressive prevention. Suppression of rights is not a governance tool — it is a violation of the rule of law. When citizens are structurally tracked, quantified, and manipulated through systems beyond their control, **there is no longer protection — only conditioning.**

If the State operates through third parties to circumvent legal safeguards. Such conduct is not only **unlawful** but also contrary to the principles of **justice and human dignity**. In this context, **slavery is redefined** as a condition in which **human dignity is undermined by structural dependence**, without a reasonable path to autonomy.

I hereby invoke the **fundamental human rights** guaranteed by the **European Convention on Human Rights (ECHR)** and the **Charter of Fundamental Rights of the European Union**, which stand above national and technological expediency.

Legal Foundations and Jurisprudence

- **Article 8 ECHR**: *Right to respect for private and family life, home, and correspondence.* → Any interference must be **in accordance with the law**, pursue a **legitimate aim**, and be **necessary in a democratic society**.
- **Big Brother Watch and Others v. United Kingdom (2021)**: The ECtHR ruled that the UK's bulk interception regime **violated Article 8**, due to lack of safeguards and oversight. The Court emphasised that **mass surveillance must meet strict necessity and proportionality tests**.
- **Centrum för rättvisa v. Sweden (2021)**: The Court reiterated that **general surveillance powers must be subject to independent oversight** and **clear legal frameworks**, especially when affecting large populations.
- **Podchasov v. Russia (2024)**: The ECtHR found that **metadata collection** can be just as intrusive as content interception, and must be treated with equal legal scrutiny.
- **EU Charter Article 1**: *Human dignity is inviolable.* → Any system that reduces individuals to data points or behavioural profiles **violates the essence of human dignity**.

In light of the foregoing legal analysis, including references to both European and domestic legislation, it must be emphasised:

You are executing policies on behalf of a party with whom I hold no contractual, legal, or constitutional relationship. Should you persist in this conduct, you thereby position yourself as an extension of governmental coercion.

This position is supported by jurisprudence underscoring the autonomy of private agreements and the legal principle that no third party, including the State, may impose obligations outside the bounds of lawful authority or mutual consent. Any continued enforcement of externally imposed rules constitutes a breach of the fundamental right to private self-determination and freedom from unlawful interference.

With respect, **[Your Full Name]**

Date: August 6, 2025

GDPR, data privacy, personal data, data protection law, privacy rights, digital privacy, data governance, biometric surveillance, facial recognition, AI monitoring, mass surveillance, biometric data, digital profiling, algorithmic bias, human rights, digital ethics, legal analysis, regulatory compliance, civil liberties, tech policy, European Union, Netherlands law, EU regulation, Dutch privacy law, international law